JPKI Security Certification scheme for Mobile Devices, version 1.0

1 Introducing the scheme

The JPKI Security Certification scheme for Mobile Devices (JPKI-MD) is used by Digital Agency to have implementers of the JPKI specification demonstrate that a specific product protects the assets in the JPKI-compliant product against state-of-the-art attackers.

This document describes the security evaluation and certification process to be followed.

1.1 Platform and product overview

This scheme applies to a TOE implementing JPKI functionality such as PKI products.

1.1.1 JPKI product

This scheme applies to a platform and an applet (the JPKI Applet) composed on JPKI product.

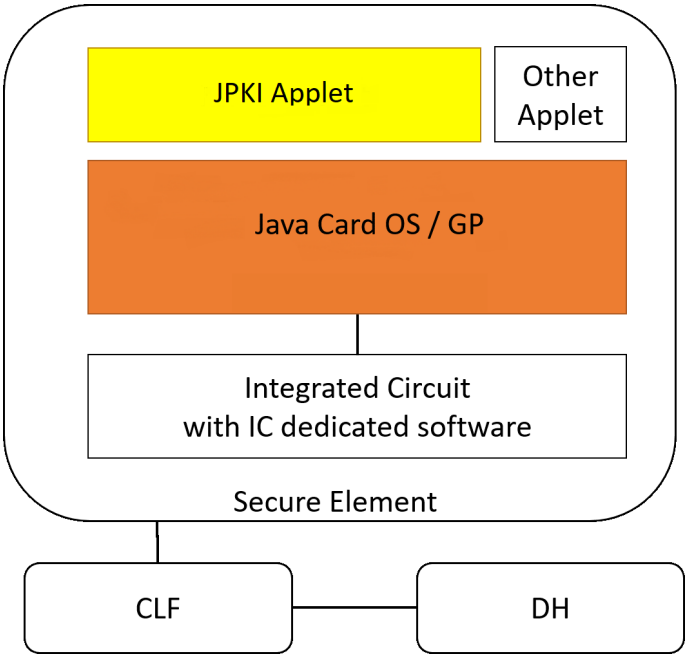


Figure 1-1: Overview of JPKI product

In this scheme, the TOE for JPKI Applet:

- JPKI Applet, depicted in yellow in the picture.

These components are composed in the order shown here, on top of a hardware and the Java Card platform. Requirements stated in the scheme documentation apply to all components unless explicitly stated otherwise.

The functional and assurance requirements depend on the JPKI functionality implemented, as described in the appropriate Protection Profile (PP):

- JPKI Applet Protection Profile [JPKIPP]

Any evaluation under the JPKI-MD scheme shall be against the appropriate PP(s), by providing the ST compliant to those PP(s).

1.2 Intended audience

This document is intended for the following involved parties:

1. Scheme owner (Digital Agency)
2. Developer (GP-SE vendor)
3. Evaluator (Lab)
4. Certifier (TrustCB)
5. Applet developer

1.3 Terminology

The terminology of RFC 2119 is used in this document, as follows:

- “shall” or “must” indicates mandatory requirements
- “should” indicates a strong recommendation, deviation of which must be discussed with and approved by the scheme
- “can” or “may” denotes an option

1.4 Reference Materials

The documents listed in Table 1 may have been cited in this document or used to obtain background information.

Table 1. Reference Documents

Title	Reference
Joint Interpretation Library Application of Attack Potential to Smartcards https://www.sogis.eu/uk/supporting_doc_en.html	[JIL]
ISO Standard 15408 Common Criteria for Information Security Evaluation Common Criteria and CEM standards.iso.org or commoncriteriaportal.org	[CC]
EMVCo Security Evaluation https://www.emvco.com/	[EMV]

Title	Reference
ETR for composite evaluation template https://www.sogis.eu/documents/cc/domains/sc/JIL-ETR-template-for-composition-v1-2.pdf	[ETR-tmpl]
JPKI Applet Protection Profile https://www.ipa.go.jp/en/security/jisec/pps/certified-cert/C0859_it5919.html	[JPKIPP]
BSI-CC-PP-0099 Java Card System – Open Configuration Protection Profile https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/pp0099b_pdf.pdf https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/pp0099V2b_pdf.pdf https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/pp0099V3b_pdf.pdf	[JC-PP]

1.5 Contact Names and Enquiry Procedures related to the security evaluation

All requests or enquiries should first be addressed by email to: JPKI-MD@trustcb.com.

The scheme owner can be contacted at: mynumber_smartphoneteam@digital.go.jp.

2 JPKI-MD Scheme Overview

This section provides an overview of the JPKI-MD Scheme, including the objectives of the scheme, roles and responsibilities for all parties, and a high-level description of the evaluation process.

2.1 Objective

The objectives of the scheme are:

- To protect the customer assets stored in JPKI-compliant products against threats from state-of-the-art attackers.
- To protect the JPKI service by ensuring that no insecure JPKI products appear on the market by establishing sufficient assurance that the JPKI products protect the assets against threats from state-of-the-art attackers.
- To ensure that the scheme owner Digital Agency does not obtain proprietary information from developers.

This scheme leverages and streamlines the Common Criteria [CC] evaluation process by focusing on specific threats that JPKI products are exposed to, in the context of industry standard designs and processes.

To maintain a consistent and state-of-the-art level of assurance, experienced evaluation labs are appointed to perform the evaluation activities.

A dedicated certification body (TrustCB) is appointed by the scheme owner to perform the certification activities.

2.2 Roles

There are four main roles in this scheme, as follows:

- Scheme owner: Digital Agency, operator of the JPKI-MD scheme and providing JPKI Applet.
- Developer: GP-SE vendor submitting the TOE for evaluation and certification.
- Evaluator: Lab evaluating the TOE.
- Certifier: Certification Body certifying the work of the Evaluator
- Applet developer: Applet developer submitting the evidence of the JPKI Applet

2.3 Scheme owner

Digital Agency, intending to protect the customer assets and the JPKI service, as owner of this security scheme:

shall maintain the scheme documentation and procedures.

- shall accredit the certifier.
- shall maintain the definitive list of accredited certification bodies.

- shall decide whether the usage limitations of a product are acceptable within the intended usage.
- shall make final decisions on any discussions and or escalations conflicts within the scope of this scheme.

This scheme is designed to keep proprietary information of the developer and evaluator separated from the scheme owner. Therefore, unless essential for conflict resolution, the evaluator and certifier shall not provide the scheme owner access to proprietary developer evidence or proprietary evaluation evidence, beyond the evidence submitted to the scheme owner in the due cause of the process. If there is a need to disclose proprietary developer or evaluation evidence to the scheme owner, prior explicit authorization by the developer or evaluator respectively shall be required.

2.4 Developer

The developer:

- shall arrange any contracts with the evaluator and certifier, including payment for the activity and confidentiality requirements. The developer shall support the independence and impartiality of the evaluator and certifier. The timing and amount of payment must not be dependent on the evaluation/certification outcome. The evaluator and certifier must have full access to relevant developer and evaluation evidence.
- shall apply for (re-)certification under the scheme for a specific product, by filling out the application form and sending it to the certifier.
- shall arrange that any evidence necessary is made available to the evaluator (and if necessary the certifier). This should include samples of the product, the guidance documentation of the product, the site audit result(s) (for CC: site certificates or Site-Audit Reuse Sheets/STAR reports, for EMVCo Shared Audit Report), the ETR for composition (for CC certified hardware/platforms) or the Shared Evaluation Report (for EMVCo approved hardware/platforms), and any underlying hardware/platform documentation required.
- shall NOT claim nor imply that a product is certified, before issuance of the certificate by the certifier for that exact product.
- shall NOT claim nor imply that a product is certified after expiry or revocation of the certificate.
- shall inform the evaluator of any information (including known possible weaknesses and attacks) relevant to the evaluation of the TOE.
- shall inform all parties (including the scheme owner) immediately if any vulnerability of the TOE becomes known during the validity period of the certificate. The developer may discuss possible vulnerabilities with the evaluator and certifier to determine whether they are actual exploitable vulnerabilities prior to contacting the scheme owner. Informing shall be done in a timely manner but not later than 30 days after being known to any party. Any unresolved discussion shall be taken to the scheme owner.
- shall archive the developer evidence for at least three years after expiry of the certificate.

- shall, in case of dispute over whether a product sold as the certified product is genuinely the certified product, support the verification against the stored evidence and samples, as well as any further fact finding required to resolve this.
- should inform the scheme owner of potential improvements of the scheme documentation, including the security analysis.
- shall, in case of changing production sites related to the certified products, apply for the assurance continuity to the scheme owner, and provide the Impact Analysis Report (IAR) to the certifier.

2.5 Evaluator (evaluating lab)

The evaluator is a laboratory accredited by the scheme owner for the evaluation role.

The evaluator is responsible for performing all vulnerability analysis and security testing needed to ensure that the product protects the assets against current state-of-the-art attacks.

The evaluator:

- may assist the developer in the application process.
- shall ensure the evaluator's independence of the developer, the certifier and the scheme owner.
- shall ensure that the same lab shall perform both applet pre-evaluation and main evaluation.
- shall determine whether the developer evidence provided meets the requirements as set in the scheme documentation.
- shall provide the certifier with a test plan.
- may await approval by the certifier prior to testing (proceeding without approval runs a risk of testing not being judged sufficient, at the potential time and costs risk of the evaluator/developer).
- shall inform the developer of the fact the test plan has been submitted to the certifier.
- shall perform all vulnerability analysis and security testing needed to ensure that the samples of the product protect the assets against the current state-of-the-art attacks as defined in the applicable protection profile.
- shall answer the questions from the certifier.
- shall provide the applet developer and the certifier with JAIR describing the evaluation activities and conclusion that the product meets the requirements.
- shall provide the developer and the certifier with the ETR describing the evaluation activities and conclusion that the product meets the requirements.
- may provide the developer with extra details on the test results outside the scope of this process.
- shall inform all parties (including the scheme owner) immediately if any vulnerability of the TOE becomes known during the validity period of the certificate. The developer may discuss possible vulnerabilities with the evaluator and certifier to determine whether they are actual exploitable vulnerabilities prior to contacting the scheme owner. Informing shall be done in a timely manner but not later than 30 days after being known to any party. Any unresolved discussion shall be taken to the scheme owner.

- shall archive the developer evidence, evaluation evidence and samples for at least three years after expiry of the certificate. Note that the raw measurement data is not considered evaluation evidence and hence is excluded from the archiving requirement.
- shall, in case of dispute over whether a product sold as the certified product is genuinely the certified product, perform the verification against the stored evidence and samples.
- should inform the scheme owner of potential improvements of the scheme documentation, including the security analysis.

2.6 Certifier (Dedicated Certification Body)

The certifier is a dedicated certification body accredited by the scheme owner for the certification role. Digital Agency has accredited TrustCB as the certification body for the JPKI-MD scheme.

The certifier is responsible for determining whether sufficient assurance has been given that the product protects the assets against current state-of-the-art attacks, and issuing a certificate to that effect, without disclosing proprietary information of other developers to scheme owner.

Note that the certifier makes this critical decision on behalf of the scheme owner, because the scheme owner will normally copy this decision without further discussion.

The certifier:

- shall maintain its impartiality.
- shall accredit and maintain the definite list of evaluators (evaluating laboratories).
- may assist the developer in the application process.
- shall ensure the certifier's independence of the developer and the evaluator involved in this project.
- shall verify the certification application form meets the requirements of the scheme documentation, and shall issue an intended certification ID.
- shall determine whether the proposed test plan of the evaluator will likely provide sufficient assurance in testing.
- shall inform the developer and the evaluator of the approval of the test plan.
- shall verify that the ETR and JAIR meets the requirements as documented in the scheme documentation.
- should ask questions to the evaluator if it is not clear to the certifier whether sufficient assurance has been achieved.
- shall determine whether sufficient assurance has been given that all vulnerability analysis and security testing needed to ensure the product protects the assets against the current state-of-the-art attacks.
    - If the certifier determines sufficient assurance is given, the certifier shall send a certificate with the certification ID to the developer, the evaluator and the scheme owner.
    - If the certifier determines that insufficient assurance is reached even after questions to the evaluator, the certifier shall inform the developer and the evaluator of this verdict.

- shall maintain the list of current valid certificates.
- shall in all cases inform both the developer and the evaluator of the verdict.
- shall inform all parties (including the scheme owner) immediately if any vulnerability of the TOE becomes known during the validity period of the certificate. The developer may discuss possible vulnerabilities with the evaluator and certifier to determine whether they are actual vulnerabilities prior to contacting the scheme owner. Informing shall be done in a timely manner but not later than 30 days after being known to any party. If the certifier has reasonable suspicion during the assessment that the product fails to protect the assets against now current state-of-the-art attacks, the certificate should be suspended. If the certifier determines that the product fails to protect the assets against now current state-of-the-art attacks, the certificate shall be revoked. Any discussion unresolved after at most 30 days shall be taken to the scheme owner.
- shall, in case of dispute over whether a product sold as the certified product is genuinely the certified product, confirm or deny the verification against the stored evidence and samples by the evaluator.
- shall inform the scheme owner of potential improvements of the scheme documentation, including the security analysis.
- shall, in case of changing production site related to the certified product, review the IAR provided by the developer and make decision whether maintenance or re-evaluation (delta) process is appropriate.

2.7 Applet Developer

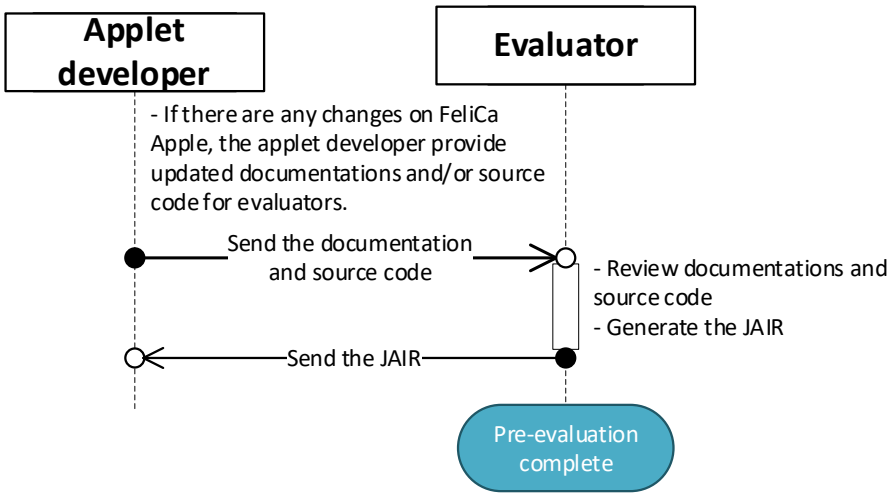
Applet developer:

- shall provide pre-compiled evidence to which evaluator and certifier need to perform their activities. Pre-compiled evidence is defined in chapter 3.

3 Process

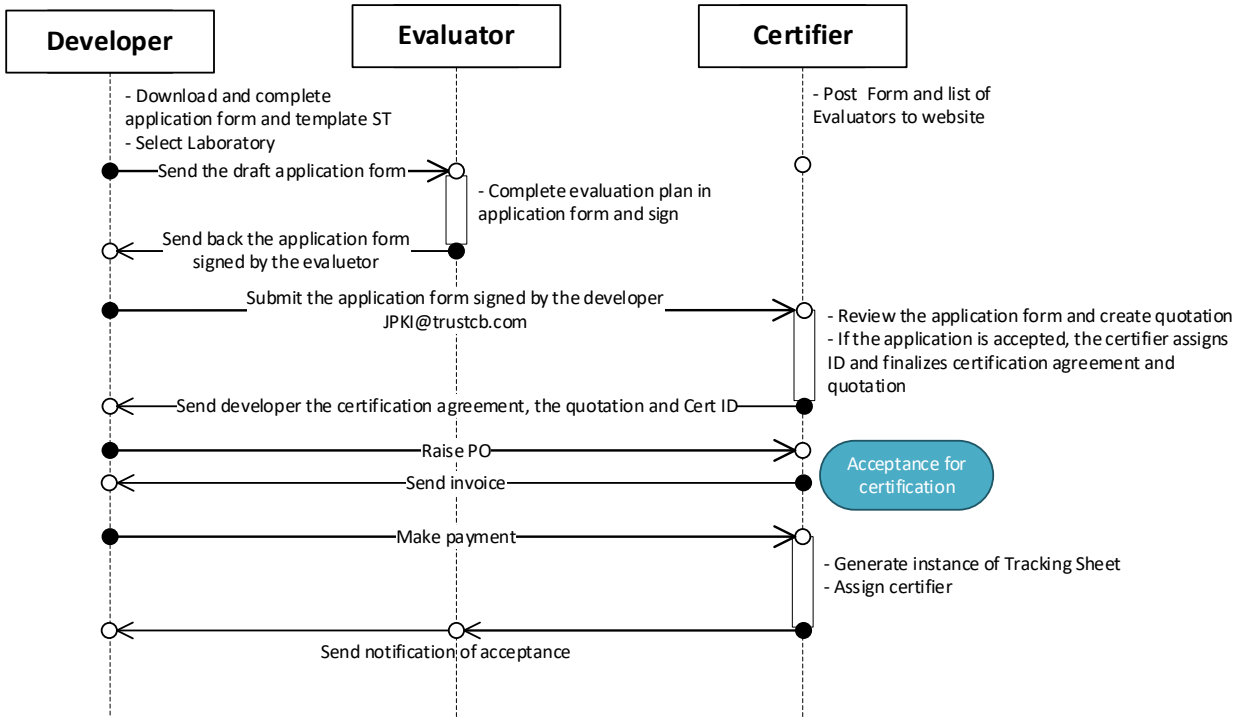
3.1 Applet pre-evaluation phase

In the pre-evaluation phase, the evaluator reviews documents and source code of the JPKI Applet. And the, the evaluator generates JPKI Applet Intermediate Report (JAIR). The JAIR will be submitted with ETR during Main Evaluation phase.



3.2 Submission for Main Evaluation phase

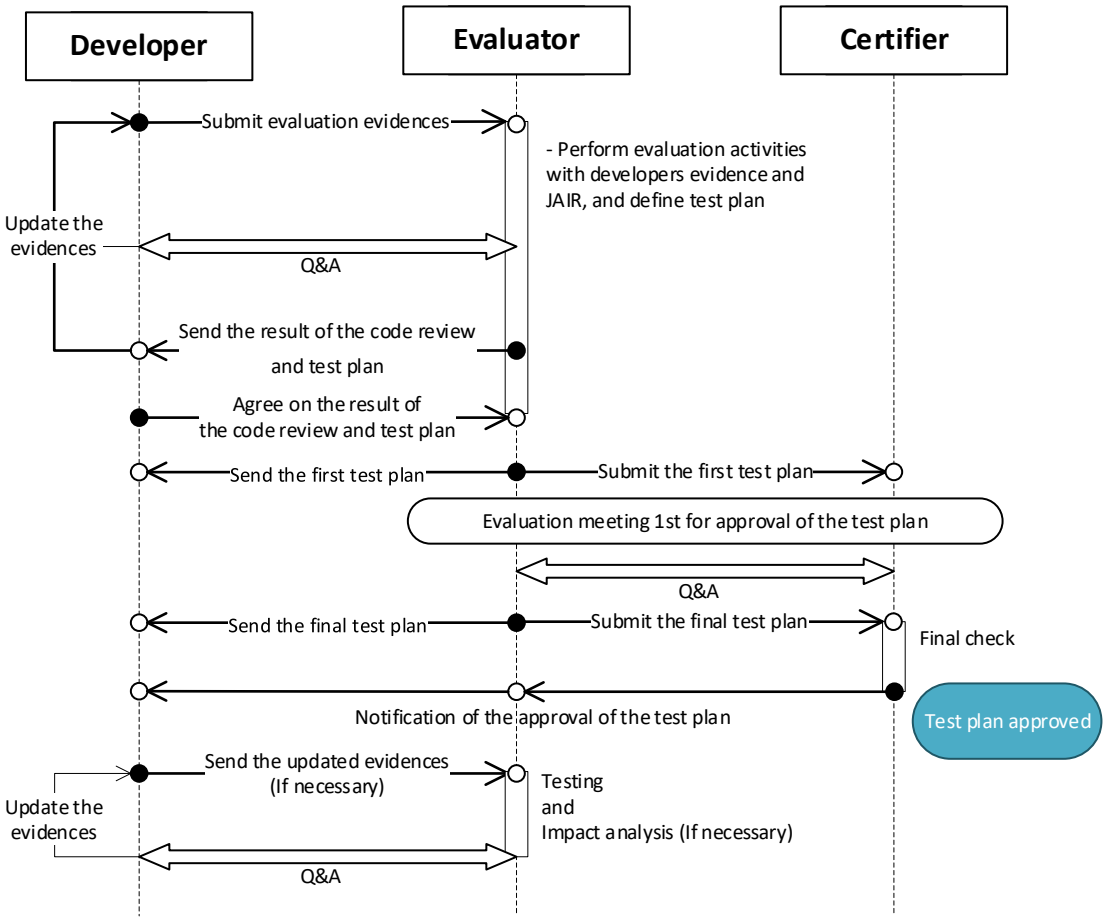
In the submission phase, the developer arranges the application and any contracts with the evaluator. When successfully completed, the evaluation and certification process has started and the intended certification ID is communicated.



If the certifier determines that an adaptation of the existing scheme procedures or evaluation methodology is needed because the TOE type, scope or other aspects don't match, or for other reasons additional oversight by the certifier be required, a kickoff meeting and/or other additional meetings may be required.

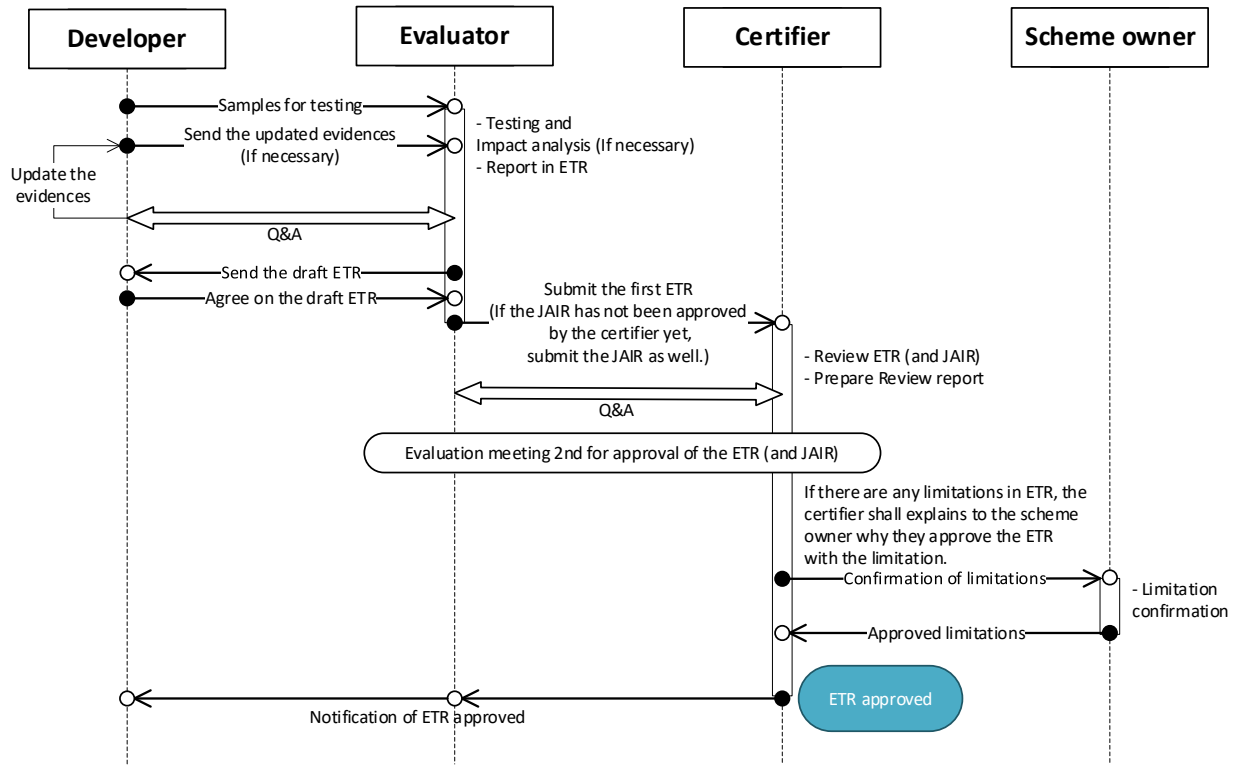
3.3 Main Evaluation phase (vulnerability analysis and test plan)

In the evaluation phase, the evaluator reviews the source code and any other needed information, and generates the vulnerability analysis and test plan. This is discussed with the certifier and, if sufficiently clear that it will lead to sufficient assurance, the certifier will approve the Test Plan.



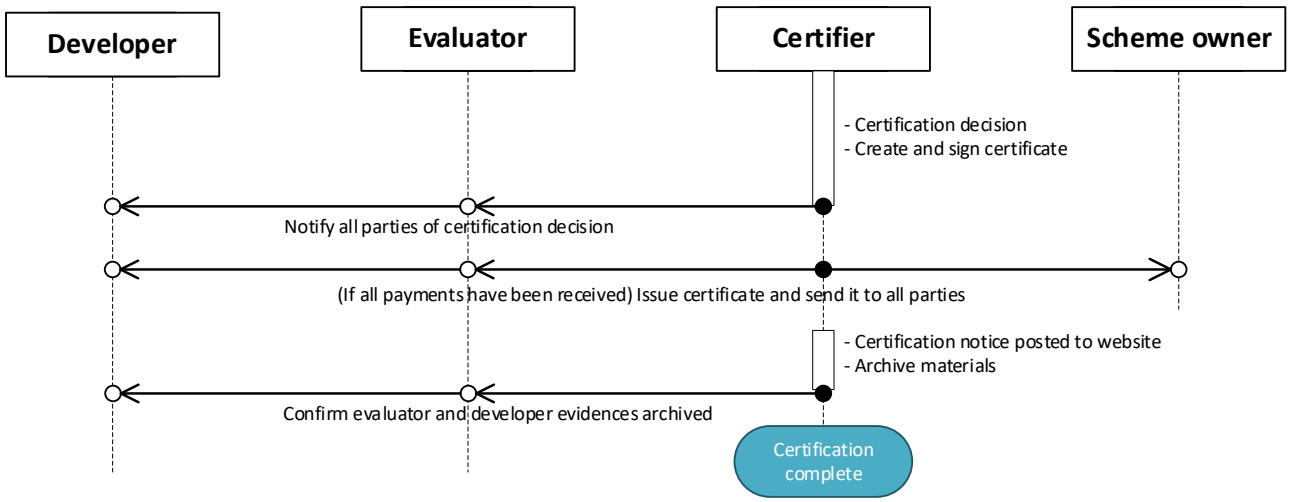
3.4 Main Evaluation phase (test results)

After testing, the evaluator will generate the ETR, may discuss it with the developer, and then presents the ETR and the JAIR to the certifier. If the certifier considers the results to be sufficiently convincing, he will issue a certificate.



3.5 Certification phase

After acceptance of the ETR and the JAIR, the certificate will be issued.



3.6 Optimized guidance per assurance activity

In applying the CC assurance activities on a given TOE, the PP contains mandatory application notes. These application notes allow for optimizations in the assurance activities approved by the scheme owner. There are three categories of scheme activities:

1. "Already performed at scheme level": These assurance activities have already been performed at scheme level and should not need to be repeated in a given evaluation. The evidences verified at that time are provided as pre-compiled evidences for all evaluators. If a need to perform this activity is perceived, the scheme owner shall be contacted as it may indicate an oversight in the scheme processes or misunderstanding in the requirements of this scheme.
2. "Verification of variable part only": These assurance activities require only minor verifications by the evaluator.
3. "Examination": These assurance activities require examination by the evaluator.

Previous version JPKI-MD scheme	Traditional CC	Current JPKI-MD scheme		
		Already performed at scheme level	Verification of variable part only	Examination
	ASE ASE_COMP		X	
JPKI specification	ADV_FSP	X		
	AGD_OPE	X		
	AGD_PRE	X		
Design description (verbal/presented)	ADV_ARC	X		
	ADV_TDS	X		
Source code review	ADV_IMP			X
	ADV_COMP			X
Compliance testing	ATE_COV ATE_DPT	X		
	ATE_FUN ATE_COMP			X
Vulnerability analysis	AVA AVA_COMP			X
Process	ALC ALC_COMP		X	

As can be seen, the evaluation is expected to be lightweight by verifying that the expectations of an industry-standard design (ASE, ADV_FSP, ADV_TDS, ADV_ARC, AGD, ATE) and procedures and sites (ALC) are warranted for this TOE, and in depth to focus on code review (ADV_IMP) for vulnerability analysis (AVA).

3.7 Documents and authorized recipients

The table below describes which documents are created by whom, and who shall or may receive them as a result of this process. In the table body, **bold** indicates the named party or parties responsible for generating the document.

	Developer	Evaluator	Certifier	Scheme owner	Applet developer
Application form	**M**	M	M	M	-
Applet evidence for pre-evaluation	-	M	O	**-**	**M**
Developer evidence	**M**	M	O	-	-
JAIR	-	**M**	M		M
Communication of evaluator to certifier	O	**M**	M	-	-
Test plan	M	**M**	M	-	-
ETR	M	**M**	M	-	-
Usage limitations	**M**	**M**	M	M	-
Optional extra reporting to developer	O	**O**	O	-	-
Certificate	M	M	**M**	M	-
Project progress information	**M**	**M**	**M**	-	-

M = mandatory

O = optional

- = NOT AUTHORIZED to receive

4 Certificate validity

A new certificate is valid for a period of 5 years from the ETR issue date.

When the certified product is modified, a new certificate is required. If the same evaluator has performed an earlier evaluation of the same product or can determine the limited impact of changes in the product or underlying hardware/platform compared to a previously certified product, then the evaluator may internally re-use prior analyses and test results. This process can lead to maintenance or recertification process.

In case of recertification, the evaluator needs to re-evaluate the product in order to assess again the assurance level. The resulting analysis and testing shall always show that the product protects the assets against current state-of-the-art attacks and current rating methodology [JIL]. As a result, of recertification, the new certificate is valid for a period of 5 years. All tests (re-)used for the analysis should not be more than 6 months older than the ETR issue date. Any tests (re-)used that are older than 6 months but no older than 12 months may be (re-)used only with the explicit approval of the certifier. No tests used for the analysis should be more than 12 months older than the ETR issue date.

In case of maintenance, minor changes (typically non-TSF) do not have impact on the assurance level gained in the original evaluation and the validity of the new certificate is linked to the original product certificate date. In this case, evidences that the functional testing has been updated or in case of a very minor change, a statement that the old functional testing is still valid for the updated TOE.

JAIR is valid for a maximum period of 30 months from JAIR issue date. The evaluator can reuse the evaluation work presented in the JAIR as long as there are no changes to the JPKI Applet and the ALC results reported are still valid. JAIR reuse is only possible within the same Lab.

4.1 Composition aspects: re-use of other certificates

4.1.1 Composition aspects for JPKI product

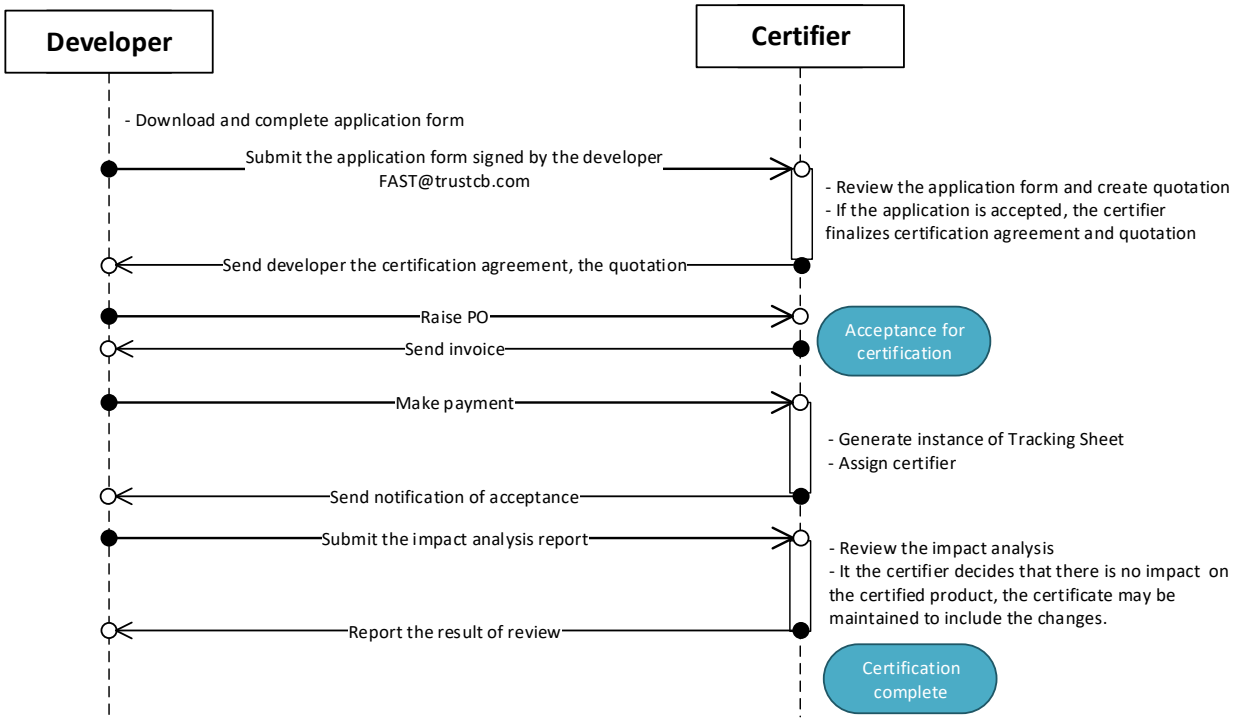
A certificate for the underlying platform as a Java Card platform can be re-used only if there is a valid Common Criteria certificate against Java Card System PP [JC-PP] at AVA_VAN.5, or EMVCo approved platform. The scope of the Java Card Platform must include GlobalPlatform card management functionality needed for the JPKI Applet, including GlobalPlatform amendment C and D. The Java Card Platform certificate shall be at most 1.5 years old at the time of issuance of the ETR in case of CC, or 1 year old in case of EMVCo.

If there are different versions of the underlying guidance of the platform parts, all versions must be considered. If the evaluator determines that the changes in the guidance have no security impact on the composition, the certifier may accept this determination as sufficient. Otherwise, extra analysis and testing of the composition should be performed.

4.1.2 Re-use policy of the site evaluation

All sites involved in the development and production (including all sites involved in the loading of plaintext code of the JPKI specific components, excludes encrypted loading of the JPKI specific components and the personalization of the applet) must be audited in compliance to the applicable requirements from those Common Criteria or EMVCo requirements. The site audits can be reused from the date of the site audit according to the former SOG-IS or a successor approach.

Changes to the production sites shall be reported to the certifier with an impact analysis. If the certifier can determine that there is no impact on the product, the certificate may be maintained to include the new sites, and the certifier reports to the developer.



5 Reporting (Evaluator): JAIR

5.1 Objective

The reporting from the evaluator to the certifier is intended to provide the certifier with sufficient information to determine that enough assurance has been gained, without disclosing more proprietary knowledge than is necessary. For this reason, the industry standard Common Criteria ETR or EMVCo reporting shall be used, as this is a common format of documents already exchanged between these stakeholders in the course of CC and EMVCo evaluations.

5.2 Requirements

The evaluator shall use the Evaluation Technical Report for Composition template of SOGIS [ETR-tmpl] or EMVCo report as basis for the reporting. Note that this document shall not be sent to the developer.

Note also that this document is considered to contain sensitive information about the security and potential security weaknesses of the product and therefore shall be kept strictly confidential.

The version of this JPKI-MD scheme document applied shall be stated.

5.3 Evaluation results

The evaluator shall explicitly state:

- that the evaluator has determined that the JPKI Applet meets all requirements of the JPKI-MD scheme.
- any significant limitations on the use of the TOE.

5.4 Maintenance

The evaluator shall update the JAIR when:

- The source code of the JPKI Applet is updated, or
- The ALC result of the JPKI Applet is updated.

6 Reporting (Evaluator): ETR

6.1 Objective

The reporting from the evaluator to the certifier is intended to provide the certifier with sufficient information to determine that enough assurance has been gained, without disclosing more proprietary knowledge than is necessary. For this reason, the industry standard Common Criteria ETR or EMVCo reporting shall be used, as this is a common format of documents already exchanged between these stakeholders in the course of CC and EMVCo evaluations.

6.2 Requirements

The evaluator shall use the Evaluation Technical Report or EMVCo report as basis for the reporting. Note that this document shall not be sent to the scheme owner.

Note also that this document is considered to contain sensitive information about the security and potential security weaknesses of the product, and therefore shall be kept strictly confidential.

The evaluator shall report his findings in the form of an ETR, and include all certificates, Shared Evaluation Reports, Shared Audit Reports and other evaluation evidence used in the reference list in the ETR.

The version of this JPKI-MD scheme document applied shall be stated.

6.3 Evaluation results

The evaluator shall explicitly state:

- that the evaluator has determined that the product meets all requirements of the JPKI-MD scheme.
- any significant limitations on the use of the TOE.
- that the evaluator advises the certifier to certify the product, by concluding that the evaluator “has determined that the product meets the requirements of the JPKI-MD scheme procedures and has high-assurance that the product protects the assets against state-of-the-art attackers according to [JIL] at the time of issuance of this report”.

7 Reporting (Certifier): Certificate

7.1 Requirements

To protect the scheme owner's brand and assets, the certifier shall decide whether or not the requirements of the PP have been met and hence a sufficiently high level of assurance has been obtained to ensure that the TOE protects assets against state-of-the-art attacks according to [JIL].

The certifier shall verify that the evaluator's ETR and JAIR meets all requirements set in the scheme documents.

If the certifier has decided that sufficient assurance is gained that the product is shown to protect the assets, and all requirements in the scheme documentation are satisfied, then the certifier shall issue the certificate using the Certificate Template.